

**SEALED**

United States District Court

NORTHERN

DISTRICT OF

AUG 18 2016

CLERK, U.S. DISTRICT COURT  
By TEXAS  
Deputy *[Signature]*

**In the Matter of the Search of**  
(Name, address or Brief description of person, property or premises to be searched)  
THE RECORDS OF GOOGLE, INC.,  
1600 AMPITHEATRE PARKWAY,  
MOUNTAIN VIEW CALIFORNIA,  
ASSOCIATED WITH THE ACCOUNT  
GO4BRYCE@GMAIL.COM

**APPLICATION AND AFFIDAVIT  
FOR SEARCH WARRANT**

**CASE NUMBER:** 3:16-MJ-668-BN

I Jason Ford being duly sworn depose and say:

I am a Task Force Officer with the U.S. Drug Enforcement Administration and have reason to believe that on the property or premises known as (name, description and/or location)

See Attachment A, incorporated herein.

in the NORTHERN District of CALIFORNIA there is now concealed certain property, namely (describe the property to be seized):

See Attachment B, incorporated herein.

**which is** (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

evidence of a crime, fruits of a crime, and property designed for use, intended for use, and used in committing a crime.

**The facts to support a finding of Probable Cause are as follows:**

(SEE ATTACHED AFFIDAVIT OF JASON FORD).

Continued on the attached sheet and made a part hereof. XX Yes    No

*Jason Ford*  
\_\_\_\_\_  
Signature of Affiant

JASON FORD

Task Force Officer, DEA

**Sworn to before me, and subscribed in my presence**

August 18, 2016  
Date

at

Dallas, Texas  
City and State

DAVID L. HORAN  
United States Magistrate Judge  
Name and Title of Judicial Officer

*[Signature]*  
\_\_\_\_\_  
Signature of Judicial Officer

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Jason Ford, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a Dallas Police Officer assigned to the Narcotics Division. I have been a police officer for 25 years, and assigned to Narcotics for 13 years. I am also a Task Force Officer (TFO), with the Drug Enforcement Administration (DEA), assigned to Dallas, Texas. I have been a TFO for more than 12 years.
2. I have attended classes and courses conducted by the DEA, the U.S. Attorney's Office, and other government agencies regarding the conduct of various criminal activities by persons and/or groups who illegally import, distribute and sell illegal narcotics. I have participated in a number of drug trafficking, money laundering, and organized crime investigations conducted by the DEA and other law enforcement agencies, which resulted in the arrest of numerous subjects, the seizure of property and assets, and the seizure of controlled substances. As a result of my training and experience, I am familiar with how persons and/or groups who illegally import, traffic, distribute, and sell narcotics use various criminal enterprise schemes to conduct their activities. I have also directed, supervised or participated in numerous searches of residences and businesses of suspected drug traffickers for evidence of criminal activity.
3. I have also become knowledgeable in the enforcement of state and federal laws pertaining to narcotics and dangerous drugs. Based on this experience, I have become well-

versed in the methodology utilized in narcotics trafficking operations, the unique trafficking patterns employed by narcotics organizations, and their patterns of drug distribution. I have also interviewed convicted drug dealers on numerous occasions. Based upon this experience, I have become knowledgeable of the methods and modes of narcotics operations and the language and patterns of drug abuse and trafficking, including the related money laundering.

4. I am also familiar with the use of social media and electronic communication by criminals to communicate with each other for purposes of drug distribution.

5. I make this affidavit in support of an application pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), 2703(c)(1)(A), 2703(g), and Federal Rule of Criminal Procedure 41, for a warrant to search all records of Google, Inc. ("Google"), a digital information company headquartered in Mountain View, California, associated with Bryce Hansen, for evidence, fruits and instrumentalities of violations of 21 U.S.C. §§ 841(a)(1), 846 and 856(a)(1).

Specifically, I respectfully submit that based on the facts set forth below in this affidavit and the reasonable inferences arising from these facts, as well as my training and experience, there is probable cause to believe that Bryce Hansen, knowingly possessed with intent to distribute a controlled substance in violation of 21 U.S.C. § 841(a)(1), conspired with others to possess with intent to distribute controlled substances, in violation of 21 U.S.C. § 846, and maintained a drug-involved premises, in violation of 21 U.S.C. § 856(a)(1). I further submit that these facts and inferences establish probable cause to believe that evidence, fruits, and instrumentalities of these crimes, as described further in Attachment B, will be found in the Google account of Bryce Hansen.

6. The facts in this affidavit are based upon my personal observations, my training and experience, records and information obtained during the course of this investigation, and information provided by other law enforcement personnel with experience in the investigation of financial crimes. This affidavit is submitted for the sole purpose of establishing probable cause for this search warrant, and does not purport to set forth all of my knowledge about this matter or all information gathered during the course of the investigation.

**FACTS ESTABLISHING PROBABLE CAUSE**

7. On June 22, 2016, the Grand Jury returned a three-count indictment against Hansen. The indictment charges Hansen with being a convicted felon in possession of a firearm, possessing a controlled substance with intent to distribute, and maintaining a drug-involved premise. The indictment stems, in part, from guns, chemicals involved in the manufacture of gamma hydroxybutric acid, and methamphetamine that were found at Hansen's apartment and in a storage locker that Hansen rented.

8. During a proffer session with Hansen, Hansen explained to law enforcement that he communicated and/or was friends with several individuals who were involved with drug distribution, including at least one friend who he communicated with via Google+ in connection with the distribution of a controlled substance.

9. During the proffer session, Hansen stated that he maintained Google+ account through Google: go4bryce@gmail.com. Hansen also gave law enforcement written consent for law enforcement to search this Google account.

10. On or about June 28, 2016, a request was sent to Google requesting that it preserve all records and information related to the Google account: go4bryce@gmail.com. I believe that this account is associated with defendant Hansen. In general, an email that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google servers for a number of months or years. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

11. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("email") access, to the public. Google allows subscribers to obtain email accounts at the domain name gmail.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

12. A Google subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and

experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files. Google also allows their subscribers through their Google account access to a social networking site titled "Google+".

13. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

14. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet

Protocol address (“IP address”) used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

15. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.

16. As explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account

at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

17. As set forth above, and based on my training and experience, I know that information stored in a Google account may provide evidence of the "who, what, why, when, where, and how" of the offenses under investigation and further the government's ability to prove these offenses or, alternatively, to exclude the innocent from further suspicion. Therefore, the computers of Google are likely to contain evidence, fruits, and instrumentalities of the offenses under investigation, including (but not limited to) stored



electronic communications and information concerning the specified user and his access to and use of his Google email account.

18. Based on the forgoing, I request that the Court issue the proposed search warrant.

Because the warrant will be served on Google who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Search and Seizure of Digital Evidence

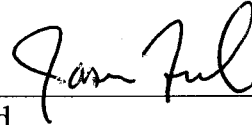
19. This Court has jurisdiction to issue the requested warrant because it is a “court of competent jurisdiction” as defined by 18 U.S.C. § 2711. Specifically, this Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

20. I anticipate executing this warrant under the Electronic Communications Privacy Act. See 18 U.S.C. §§ 2701 – 11. Under this Act, the presence of a law enforcement officer is not required for the service or execution of this warrant. 18 U.S.C. § 2703(g), The Act, in particular sections 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), authorize the Court to issue a warrant requiring Google to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

**CONCLUSION**

Based on the forgoing, I request that the Court issue the proposed search warrant.

Respectfully submitted,



\_\_\_\_\_  
Jason Ford  
Task Force Officer  
U.S. Drug Enforcement Administration

Subscribed and sworn to before me on August 18, 2016.



\_\_\_\_\_  
HONORABLE DAVID L. HORAN  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**  
**Property to Be Searched**

This warrant applies to information associated with go4bryce@gmail.com that is stored at the premises owned, maintained, controlled, or operated by Google, Inc., a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California.

**ATTACHMENT B**  
**Particular Items to be Seized**

**I. Information to be disclosed by Google**

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, including any emails, messages, records, files, logs, or information that have been deleted but are still available to Google, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- (a) The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- (b) All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- (c) The types of service utilized;

- (d) All records or other information stored at any time by an individual using the account, including Google+ information, address books, contact and buddy lists, calendar data, pictures, messages, and files;
- (e) All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes evidence, fruits, or instrumentalities of violations of 21 U.S.C. §§ 841, 846, and 856 including, for the account listed on Attachment A, information pertaining to the following matters:

- (a) The manufacture or distribution of a controlled substance, any conspiracy regarding the same, or the maintaining of a drug-involved premises.
- (b) All records discussing or relating to financial accounts, assets, or transactions;
- (c) All contact lists or address books lists associated with the account listed in Attachment A.
- (d) All communications, including but not limited to Google + communications, e-mail, chats, and instant messages, to or from the account listed in Attachment A referencing or discussing any matter referenced above;

- (e) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (f) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- (g) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).